ISSN: 1365-0653

International Journal of FORENSIC COMPUTING

Contents

JANUARY 1997

Issue 1

Advisory Board

- John Austen
  Computer Crime Consultants Ltd & Royal Holloway College, University of London, UK
- Jim Bates
  Computer Forensics Ltd, UK
- Alexander Dumbill
  King Charles House Chambers, UK
- Ian Hayward
  Department of Information Systems, Victoria University of Technology, Australia
- Robert S Jones
  Computer Related Crime Research Centre, Queen Mary & Westfield College, University of London, UK
- Nigel Layton
  Quest Investigations Plc, UK
- Stuart Mort
  DRA, UK
- Michael G Noblett
  Computer Analysis Response Team, FBI, US
- Gary Stevens
  Ontrack Data International Inc, US
- Edward Wilding
  Network Security Management Ltd, UK
- Ron J Warmington
  Citibank NA, UK

Editorial Team

- Sheila Cordier
- Ray Hatley
- Marie Easom
- Paul Johnson
- Jo Collard
  Design & Layout

Introduction

International Journal of Forensic Computing

The global increase in computer ownership is reflected in the increased incidence of computer crime which is now threatening virtually every aspect of society.

Computers have been a part of our lives for the past twenty years, but, having enabled incredible scientific and technological advances, and having been the means of establishing international communications via the Internet - they are now the weapon used by countless cyber-criminals to attack the very culture which made them possible.

Society needs to develop techniques and strategies for dealing with computer crime. The future of forensic computing lies firmly in the hands of those able to understand and implement the new laws that are arising.

The *International Journal of Forensic Computing* (IJFC) is a forum to report on and discuss all aspects of computer crime, including the techniques and technical standards which have been developed to combat it. We firmly hope that the IJFC will provide a suitable carrier for this kind of information interchange.

We would like to take this opportunity to invite readers of the journal to contribute relevant articles, and make comment on the content. Our aim is to provide a truly international view of forensic computing, and one which will stimulate and encourage the design and application of new forensic techniques. We look forward to receiving suggestions on how this might be achieved. ■

All rights reserved. Without prior permission of the Publisher, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise.

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by the Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal in relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course of action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team or members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save in respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither the Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors in articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to the Publisher.

Insight

The Royal Military Police Computer Forensic Unit

Lt. Col. Ian Waters, MBE

The Specialist Operations Unit of the British Army based at Joint Services HQ, Germany, is currently establishing a Computer Forensic Unit as part of the international fight to combat computer crime.

Headed by WO Dave Broadhead, the Computer Forensic Unit has been established to investigate any sort of computer based crime that affects soldiers or their dependants whilst they are based with the British Army in Germany.

The Unit is currently preparing for investigations which may include computer fraud, blackmail, Internet related offences and even software piracy. They are in the process of building forensic workstations and are assessing the various types of disk copying equipment on the market in the UK.

> ***WO Broadhead said: "The Military Police are subject to certain restrictions that could make a computer forensic investigation very difficult. For example, it would be impossible to impound all the hardware from a vital computer network. We are currently training our staff to use forensic disk copying equipment to make accurate copies of computer hard drives, so that work can, quickly, be resumed on a compromised system, when vital evidence has been removed for analysis."***

Providing, and substantiating, electronic forensic evidence at a court-martial is somewhat different to the civilian forensic task. Because the Army uses an enormous number of vital, and task specific, computers in its general administration work, it is not practical to remove those machines from service - even if they have the potential to provide electronic forensic evidence.

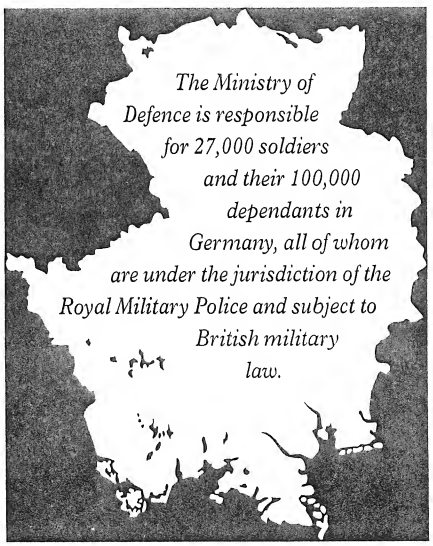
It is essential, in this situation, to copy the contents of the machine's hard drive in such a way, that the data held there is not compromised or destroyed.

Evidence gathered in this way is considered acceptable at a court-martial, and the Army retains its machines without any disturbance to day to day operations.

With fifteen years experience of military computer networks, WO Broadhead has been responsible for the installation and operation of internal networks and stand alone PC sites, both in the UK and Germany. His networking experience is supplemented by an extensive knowledge of stand alone PCs, and a keen interest in the workings of the criminal mind.

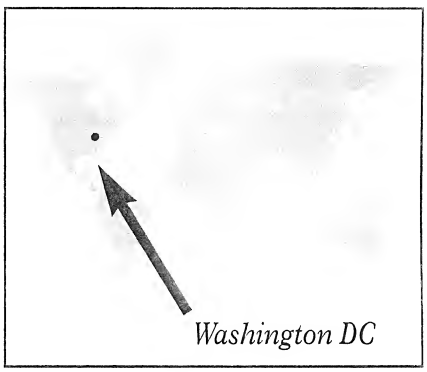
> ***Commanding Officer of HQ Specialist Operations Unit, Royal Military Police, Germany, Lt. Colonel Ian Waters, MBE said: "I have no doubt that there will be an increase in the incidence of computer crime and we are actively taking steps to ensure that computer based investigations are carried out efficiently. The establishment of a computer crime forensic investigation unit is just one of the measures we have adopted to ensure the security of military computer networks and operations."***

The British Army has adopted a severe, but eminently sensible, security policy concerning the Internet. Any machine connected to the Internet will only hold the operating system software and specific Internet related software. There will not be any connection to any other machine, neither will any other type of software be held on the Internet machine. ■



Computer Crime Scene Procedures

Any crime scene search demands that investigating officers take certain critical steps within the first few minutes. While the addition of a computer to the mix may add some technical complexity, the main issues remain security, evidence gathering, item marking, and documentation.



Washington DC

The first, and most essential, action is for law enforcement officers to secure the scene of a crime, both for their own safety and to preserve evidence. Because there may be people present with the skill, and motivation, to destroy electronic evidence, separating those people from the computer system is critical.

Forensic specialists should then attempt to determine if there is any evidence that is immediately at risk. A decision to disconnect networks or modems needs to be made quickly, and consideration should be given to the possibility that someone may be, remotely, destroying evidence.

Once these time-critical tasks are completed, areas of interest for electronic evidence need to be identified and secured. This should be carried out by a technically qualified person.

The process of identifying people who should be interviewed by technical personnel can be carried out by non-technical persons. Where possible, technicians identified for interview should not be questioned by unqualified staff until after their technical interview.

Technical experts are needed to interview suspects with technical knowledge. It is very easy for technicians to provide false or misleading information when they believe that their interviewer is not capable of discerning the truth.

Importance should be given to conducting the interview before physically accessing or dismantling the computer equipment. People who have responsibility for computer equipment tend to take ownership of these devices. As a result, they tend to be far less co-operative after watching someone dismantle 'their' machine.

If the computer system is running, it will be necessary to switch it off. Depending on which operating platform is in use, it may be necessary to shut down the computer using the operating system, before shutting off the power. Failure to do so can make recovery of some computer systems difficult or even impossible.

Before disconnecting or disassembling any computer components, everything should be labelled or tagged, initialled and dated.

It is critical that the cabling be documented precisely, as all cables which connect items to be seized must be taken. Prior to removal, the cables need to be labelled with tape and/or tags to mark each end. A corresponding tape or mark is placed on the device to which it is connected.

At this point it is very useful to do close-up photography of all the connections between individual pieces of hardware. This will provide a clear exhibit of how the system was connected and labelled. It will also facilitate the reconstruction of the system in a laboratory setting.

Once the documentation of the system is complete, disassembly can begin. Generally, it is better to remove the peripherals first, and then the CPU.

Select any documentation to be taken, as well as computer related notes or pieces of paper. Be alert to possible passwords written on 'post-it' notes, scraps of paper, or inside the covers of manuals.

In searches where there are multiple computer systems, it is important to keep items from one system separate from items or components belonging to others. If pieces from several systems get bundled together, it may be difficult to separate them later.

It is important that all computer equipment be handled gently. Any disturbance may loosen connections, which will require troubleshooting. Not all fixed magnetic media is self-parking. It should be assumed that the heads on hard drives are not parked.

Each seized item should be initialled by the law enforcement officer or forensic expert, and clearly dated. This will ensure that if a single item is entered as evidence, there will be a solid chain of custody.

These procedures should be regarded as a framework for conducting searches in a computer environment, and as a basis for policy recommendations. The US Justice Department has published Guidelines for Searching and Seizing Computers which offers more detailed information. ■

From data provided by:

Mark Pollitt, Program Manager, CART, FBI

James M Nobles, Computer Specialist, CART, FBI

Michael G Noblett, Chief, CART, FBI

Forensic Principles

by Jim Bates

The Fundamentals of Computer Forensics

When attempting to describe the purpose, principles and practice of a new science it is vital that each term and each concept is defined as clearly and concisely as possible. Such descriptions must then be presented for general discussion to ensure a consensus amongst all interested parties. To this end, these articles present an introduction to some of the more general ideas and practices which define my own concept of computer forensics.

I shall begin by defining my terms - I shall define *"computer"* as any electronic device capable of processing and/or storing information and the term *"forensic"* is defined as *"of or used in courts of law"* (Concise Oxford Dictionary).

There are a number of axiomatic principles governing the collection and examination of evidence intended for presentation in a Court of Law. These apply just as much to computer based information as they do for example, to such disciplines as DNA typing, fingerprint identification or explosives analysis. However, when attempting to apply such principles to the examination of computer based information, there are some areas where the special nature of computing requires additional considerations and some change of emphasis. I have accordingly addressed these under appropriate subheadings ...

Computer Specific Considerations

The precise manner in which information is stored by computers will vary according to the media being used but it will almost invariably result in discrete changes to the granularity of the media in such a way that the changes can subsequently be examined and interpreted to recover the pattern of the original information.

For example, take a sheet of paper ruled in squares - each square may be only black or white. The stored information is contained only in the pattern occupied by the black and white squares, and is not concerned with the paper or squares themselves. Thus absolutely identical information may be stored on different substrates, marked in a different way (perhaps circles, triangles or magnetic dipoles) and with different conditions (on/off, black/white, north/south etc.).

> ***It is therefore self-evident that the media (the substrate and the type and marking of the elements) is completely independent of the information which may thus be altered without trace.***

It is this final possibility which is of so much concern to us when considering the forensic implications of electronically stored information. It is a fact that when such information is copied, there is no way to distinguish which is the original and which is the copy without reference to additional external information.

Consider a document containing text: a photo-copy (Copy A) is taken of it. Then the original document is altered and another photo-copy is taken of it (Copy B). If the alteration was done with care it may now be impossible to distinguish solely from the copies whether Copy A or Copy B is the unaltered version. The process of copying has made the textual information pure and independent of the media used for storage. This concept of "media independence" is vital when discussing the examination and analysis of computer based material. It follows that when considering media independent information, without taking external factors into account any differentiation between original and copied information is impossible. This characteristic of computer stored information has both advantages and disadvantages when considered from a forensic point of view and I shall mention these below.

Storage Specific Considerations

Within the computer system, information may be stored in a temporary, volatile, semi-permanent or permanent form. These are arbitrarily chosen terms and I define them here as follows :-

Temporary storage is that which relies upon an external power source for its maintenance and is immediately lost if that power source is removed. This would typically be information held in computer RAM chips.

Volatile storage is that which relies upon an internal power source (e.g. batteries) and is lost if that power source is removed. The main example here would be found in the CMOS hardware that most machines use to store their configuration and calendar information. On battery powered hand-held computers, the RAM area may also be included in the volatile category.

Semi-permanent storage is that where the information, once stored, is not dependent upon a power source for its continued maintenance. Such information may subsequently be changed under the appropriate operating conditions. This includes such storage devices as floppy and fixed disks, magnetic tapes, optical disks and ▶

flash RAM. Since the semi-permanent area usually constitutes the main storage capacity of a computer, this is the area where most processed data is stored. It follows therefore that this is where most forensic interest will be centred.

Permanent storage is that where once stored, the information is unchangeable by normal processing hardware. This would typically include information contained in ROM chips.

> ***It is important to identify each of these areas accurately since the permanence or otherwise of the information may assume greater or lesser importance depending upon the case under investigation.***

For example, I would classify most CD-ROM or WORM storage as semi-permanent since although they are described as Write-Once-Read-Many, in practice the write process can often be repeated and existing data altered.

> ***The majority of evidential information is found in semi-permanent storage and this may be evaluated in isolation by considering its content, location and condition.***

Content and location are the most important and should be considered together. For example if representations of the letters 'C', 'E', 'M', 'O', 'P', 'R', 'T' and 'U' are found, they may be meaningless unless their relevant locations are known and they can form simple sequential textual information like the word "COMPUTER". Alternatively, as in the extreme case of encrypted information, all or some of the content may require additional processing before its intelligence becomes plain. The combining of words into files and files into directories together with their individual locations within an overall structure may also be vital elements within the evaluation and analysis process. Areas where such location information might add significantly to the investigation could be - the content of file slack space, the presence or absence of file fragmentation, the relationship between allocated and unallocated space or the degree of match between the logical and physical sequence of allocated clusters on a disk. Each of these at some time has figured in past investigations.

The condition element takes account of the possibility that there may be some detectable media differences which, taken in conjunction with the stored data might provide additional information concerning its origin, production or usage. For example, given two floppy disks containing virtually identical data it might be possible to identify one as older by virtue of the magnetic strength of the recorded information. Similarly any track 'spillage' might also provide additional clues to origin. This is purely hypothetical and I am not aware of any instances where such techniques have been used. However, technology may be developed to enable such examination to be conducted with a reasonable degree of accuracy and the concept must be presented for consideration. More likely is the possibility that a particular disk drive might have irregularities within its mechanism which produce an identifiable "signature" of markings when the media is examined microscopically. This condition element does not blur the distinction of the media independent concept, it simply has the potential to add more information. ■

Further sections in part 2 in the next issue of the Journal are:-

Forensic Considerations and
Considerations for the Courts.

Jim Bates, BSc (Eng) FIAP (Cmpn), President of the Institution of Analysts and Programmers, UK.

International Comment

The National White Collar Crime Centre (NWCCC) was developed from a workgroup called The Labidicas Project, founded in the early 1970's as a way for State and Local Agencies to get assistance with 'electronic data intensive' white collar crime.

The NWCCC are now a non-profit making organisation, funded by Congress, with two general offices, the Morgantail Office at the Training and Research Institute, Illinois, and the main office in Richmond, Virginia.

Chris Sanft, based at the Training and Research Institute, is responsible for in-depth computer forensic training, and ensuring that investigation agency staff are aware of the often complex laws which pertain to computer crime in the United States.

"Every time you implement a search warrant you seem to find a computer. If you are called to look at a theft case there is often a computer involved somewhere; if you go in on a drug case, you almost always discover a computer link-up. In US based crime inquiries, a computer frequently forms a part of the picture.

> ***People are finally realising the problems and questions which come as part of computer crime investigations; even businesses are realising the issues concerning electronic mail, and data theft.***

Internet access is causing some major industry problems too; certain companies have even felt the need to fire some of their top engineers for downloading pornography.

Companies and corporations are coming to understand that you have to be able to keep track of electronic information. It has even become important to consider what might happen if an ex-staff member comes back and sues you, six months after their dismissal for an electronic data crime, and you don't have the computer data which formed the evidential basis of the dismissal.

In the United States of America, all 50 states currently have computer crime legislation. However, many older laws have needed to be changed. One point which came under consideration, was the size of the penalties to be imposed - primarily, there was concern that effort be made to ensure they are severe enough. It should be noted here, that different states have different policies, but most penalties are still dependent on the perceived severity of the crime.

Unfortunately, it is not possible to implement a unified legal system in the United States, we just cannot work that way. There are, however, federal laws which apply to a lot of computer crimes if they cross state boundaries, or if a national interest computer is involved - they are frequently involved if the crime affects the banking industry.

Currently, our most serious problem, in the United States, is the overall lack of trained computer forensic investigators, which is why a lot of the work is now being carried out by the state and local agencies. This is not because they have more man power, but because the federal government does not have the resources to investigate the increasing number of computer based crimes."

This comment is compiled from an interview with

Chris Sanft

Computer Crime Training Specialist with the National White Collar Crime Centre, Illinois, USA.

Technical Tip

This month's tip comes from
Detective Constable Ian Sansome
Hampshire Fraud Squad

A little known peculiarity of Microsoft Word is the User Info feature found in the tools/options menu. This identifies MS Word documents according to the registered author but can be used to identify a document as coming from a specific machine. The feature automatically and 'invisibly' 'tags' a document header with details of the registered user for the software used to create that document. There is no obvious sign that this electronic tagging has taken place unless the document is examined with forensic software.

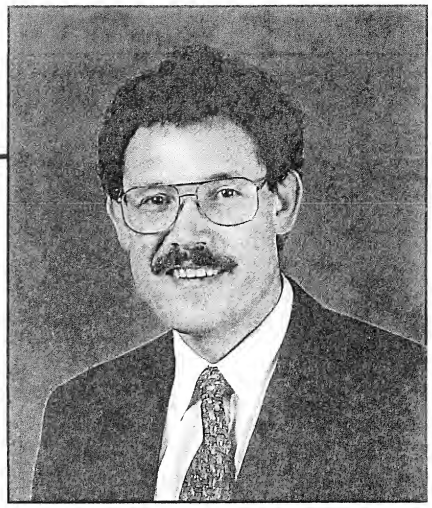
This can have a major impact on investigations which rely on positive identification of MS-Word files found on floppy disks.

Please send your tips or comments to Marie Easom at ijfc@pavilion.co.uk

Case Study

'Operation Cybertrader'

The investigation concerned distribution of child pornography via the Internet.



DI Paul Ford of Wiltshire Constabulary

Background

Information was received via the National Criminal Intelligence Service in the United Kingdom that an individual in a rural area was using the Internet to receive pornographic images of children. The individual was identified and located. Enquiries revealed that he operated a computer software business from an office at his home. It was not possible to ascertain if there were other persons employed or the type of computer equipment in use.

Search and Seizure

A search warrant was obtained from magistrates under the powers conferred by Section 4 (2) of the Protection of Children Act.

The investigating officers had not previously dealt with a crime of this nature and were concerned about the possible complexity of the computer equipment to be dismantled. Assistance during the search was therefore obtained from a computer forensic analyst.

On execution of the warrant the offender was fairly shocked and made certain admissions to police officers about his possession of indecent pictures of children. He was taken to a room at the front of the house which contained computer equipment where he was questioned by the computer forensic analyst. The purpose of the questioning was to establish:

- Which of the two computers in the room contained pornographic pictures of children.
- What operating system was being used.
- Was there a BIOS password set on the computer.
- Where was the material located on logical hard disk structure.
- What communication package was being used.
- Which Internet provider/providers were being used.
- Was the material encrypted.
- Were there pornographic pictures of children on any of the floppy disks in the room.

As a result of the questioning it was established that:

- One of the two computer systems in the room contained pornographic pictures of children.
- A number of floppy disks contained pornographic pictures of children.
- There was no BIOS password.
- The PGP encryption program was present on the machine together with public and private keys but most files were unencrypted.

Following questioning all the computer equipment in the room was seized and placed in sealed plastic evidence bags.

Also seized were 118 drawings of children engaged in various sexual activities. The suspect admitted that these were his drawings.

Whilst the search was being conducted the suspect freely admitted receiving a number of pictures of children on the Internet but avoided the issue of further distribution by himself. As a result of the admissions he was arrested and taken into custody for a preliminary interview.

Prior to the preliminary interview it was not possible to view the computer based material. During the interview the offender made numerous admissions concerning his possession of indecent pictures of children but denied further distribution. He was released on bail to report back to the police for further interview at a later date.

The Forensic Examination

Two computers were seized each containing one internal hard disk. A quantity of floppy disks were also seized. Twenty five of these were catalogued and listed by nature of sexual activity including child pornography, lesbianism, bondage and bestiality. One disk, identified by the defendant as being a collection of particularly 'hard core' pictures of children, was labelled 'Ped.Tradable'.

The seized computer material was taken to a computer forensic laboratory where it was examined. The methods used for the hard disks and floppy disks differed.

Hard Disks

One of the computers contained a 340MB hard disk and the other a 1.0GB hard disk.

The 340MB hard disk was copied using a proprietary disk image copying system which created an exact image of the original hard disk onto an optical cartridge. The image was then examined using a standard forensic workstation. Search techniques established that the hard disk contained no image files of ▶

a pornographic nature and the PC was eliminated from the enquiry.

The 1.0GB hard disk was bit copied to two sides of an optical cartridge. Using a standard forensic workstation the bit copies were reconstructed onto a hard disk of a similar capacity to the original. A search revealed that the disk contained in excess of 500 pornographic images including children. Although the PGP encryption program was present on the hard disk it had not been used and the information was easily accessible. A thorough examination of the disk was then undertaken and the communications software located. Numerous chat logs and files were found containing details of conversations with other paedophiles. Using conventional software tools, all relevant material was copied to a working optical cartridge. The graphics and chat files were examined and printed using file viewing utilities.

The copying and examination methods used for both disks ensured that the evidential integrity of the original material was maintained.

Floppy Disks

In excess of 200 floppy disks were seized of which 35 were identified as "high priority - likely to contain pornographic material". The high priority disks were image copied to an optical cartridge using dedicated forensic software. Prior to copying, the write protect tag was set on each disk in order to ensure evidential integrity. Examination of the image copies of the disks showed that there were a large number of graphic files with the files extensions JPG, BMP and GIF. A global file extraction was therefore conducted across all the floppy disk image files and those with the appropriate extensions were automatically copied to sub-directories on the working disk of a standard forensic workstation. The extracted files were then examined using a graphic file viewer.

Result of the Forensic Examination

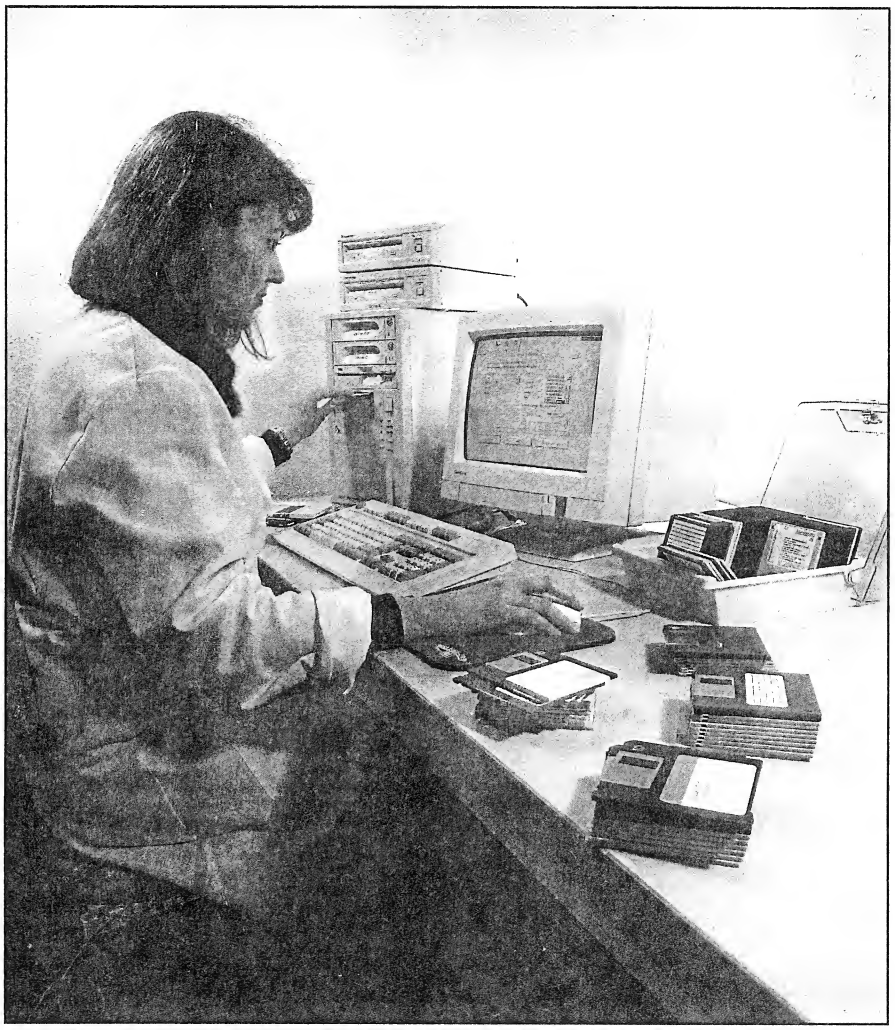
There were 1,086 graphic files on the hard disk and floppy disks. All were of a pornographic nature, many of perverse sexual activity. There were 134 images involving children of which 47 were classified as being of a 'hard core' nature.

The correspondence logs stored on the system detailed exchanges between the offender and two other persons on the Internet. These showed that there had been distribution of pornographic pictures of children. They were located in a sub-directory which also contained pornographic images. When the files in the sub-directory were arranged in date and time order it was possible to reconstruct a sequence of events that proved that there had been distribution.

The forensic examination also located material written by the defendant which took the form of personal fantasy stories. These detailed his desires to use chloroform to render unconscious and kidnap a female child aged between 7 and 9 years of age, and to carry out perverted sexual activity including torture. There was no evidence to suggest that his fantasy had become a reality.

> ***However, in a series of communication files with a female paedophile in the USA, he sought and received advice on how to procure and blackmail young children.***

The communication files also produced information that suggested that he was indecently assaulting a 9 year old girl and had ▶



Floppy disks being image copied to optical cartridge.

previously propositioned the 9 year old daughter of a former neighbour. These suggestions were confirmed in later investigations.

Due to the extremely perverse nature of the information recovered from the computer, the investigators were concerned that the accused posed a serious risk to children. A dossier was therefore printed and used in subsequent interviews. This consisted of:

- Pictures, of a most indecent nature involving children, which had been listed as 'tradable'.
- Two series of letters together with print-outs of graphics files which appeared in sequence on the hard disk communication sub-directory.
- The detailed account of his indecent assault upon the 9 year old girl.
- The account of his proposition to another child.

This dossier was produced in the formal interview with the accused. Faced with such incontrovertible evidence he made full and completely frank admissions. He was subsequently charged with possession and distribution of child pornography and indecent assault.

Case Presentation

The defendant entered a guilty plea before a magistrates' court. Prior to the court appearance discussions were held with the Crown Prosecution Service as to the means by which the computer based material could be presented. The concern was to present the material in such a way that the court would be left in no doubt as to the potential threat posed to children by the defendant. Only a small budget was available for presentation purposes and therefore any 'electronic' means was ruled out on the basis of cost. The alternative method used was to assemble dossiers consisting of photographs of the computer screen with various graphic images and communication files displayed, supported by the necessary statements of evidence. The dossiers were given to the magistrates to consider whilst the case was presented.

Outcome

The magistrates were impressed by the severe nature of the case and referred the matter to the crown court for sentencing.

The crown court found the offender guilty on the following counts:

- 2 counts of distribution of child pornography.
- 1 count of possession of child pornography with intent to distribute.
- 1 count of indecent assault.

The sentence passed was 4 months imprisonment on the first two counts, 2 months on the third and 4 months on the fourth to be served concurrently.

The prosecution lodged an appeal against the leniency of the sentence.

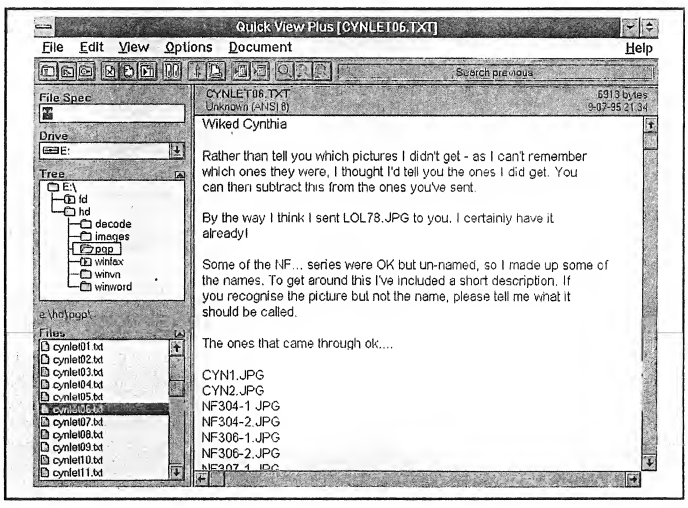
Conclusion

A number of aspects of this case are notable from a forensic computing standpoint.

- The presence of a forensic computing analyst during the search greatly assisted in narrowing the scope of the later forensic examination.
- The procedures and equipment used in the seizure, storage, copying and analysis of the computer material ensured evidential continuity and integrity.
- The examination of the material was precise and exact and all relevant information was efficiently targeted and extracted.
- *The forensic examination provided evidence to prove the initial charge and to instigate additional charges.*
- The presentation of the computer evidence in court was performed clearly and successfully within tight budgetary requirements. ■

The case study 'Operation Cybertrader' was submitted by

DI Paul Ford of Wiltshire Constabulary & Peter Verreck, Forensic Analyst.



Text of e-mail referring to file LOL78JPG containing child pornography. Used as evidence of distribution.

Book Review

'Investigating Computer Crime'

by Franklin Clark & Ken Diliberto
CRC Press, 2000 Corporate Boulevard, NW, Boca Raton, Florida 33431.
240 pp. £35.00 sterling.

Investigating Computer Crime is the latest title from CRC, the American publishing house, which specialises in all aspects of forensic science and investigation.

The strength of this book is that it is, in every sense, a practical guide. The authors have combined their personal knowledge and insights with those of many other computer crime investigators to produce a comprehensive guidebook.

There is thorough advice on the planning and preparation of search warrants, backup and interrogation software, methods to guarantee the "chain of evidence", documentation and photographic support.

Where the book is strong on procedures, search and seizure, it is less explicit or helpful on analysis and data interrogation - a number of diagnostic software packages are itemised, but little advice on how best to use this software to extract evidence.

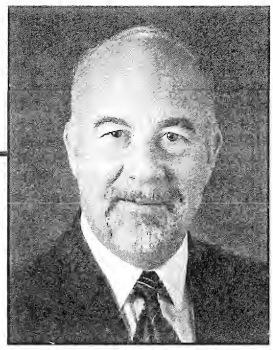
Wider aspects of computer crime are covered including a useful chapter about the on-line investigation of bulletin boards (BBS). There is also a brief but helpful introduction to PC based encryption products.

The book was written primarily for the US market and the specific information on search warrants is, therefore, of limited value to anyone operating under PACE or Anton Piller Orders. That said, the technologies, situations and solutions described are universal. Highly recommended. ■

Reviewed by: Edward Wilding
Network Security Management Ltd, London.

Profile

John Austen



John Austen - until recently the charismatic Detective Inspector in charge of the Computer Crime Unit, New Scotland Yard - is now a director of his own company, Computer Crime Consultants Ltd.

With a background in computing spanning three decades, Austen has virtual-guru status in the modern world of forensic investigation. Early work on an international banking fraud (1976) led him into the fascinating world of computer crime investigation and eventually to a post with the CCU in London.

Austen said: "In the 1980s, we recognised the capacity for crime through computers, and the need for a specialised unit, so I was given a desk and a pen, but no staff or training, to set up the Computer Crime Unit of New Scotland Yard."

Austen has come a long way since setting up the CCU in 1984. Early recognition of the potential for criminal activities within the confines of computer networks, led him to establish a training scheme for detectives to increase awareness of investigative procedures in computer based investigations.

Forensic investigation training courses have now been accepted by police at an international level, but in the early days, Austen spent much of his time talking to the 43 individual UK constabularies, teaching them to manage the process of computer based investigations.

"It is an illusion," Austen warns, "for an investigator or computer programmer to believe he can be the computer expert. People have this vision of a computer expert as a genius or a whiz-kid. The truth is that they are probably only an expert in one or two areas."

Placing emphasis on the need to consult with a variety of experts, each with specialist knowledge, has become a fundamental part of modern investigative procedure.

Austen said: "There are a number of different and specific disciplines within computing. The basic precept I laid out in the formation of the CCU acknowledges this. The same idea is central to our expert witness programme, where we identified people as experts, but only in specific areas of computing such as DOS or UNIX."

The CCU has now grown into an internationally recognised and respected team of police officers, and has had major influence in the way the British legal system regards computer crime.

From 1984 to 1996 John Austen headed the Computer Crime Unit at New Scotland Yard. He established innovative training schemes to cope with the new demands put forward by a growing computer industry, but, perhaps more importantly, persuaded the law to address computer-related crime in a way that made it understandable to those outside the industry.

Benefiting from Austen's guidance, expert witnesses were recruited from among the top industrial computer consultants. This elite band were then encouraged to develop new ways of preserving and presenting computer evidence.

More recently as Director of Computer Crime Consultants, and as a lecturer at London's Royal Holloway College, John Austen is bringing together all the aspects of forensic investigation he developed as a police officer, and is preparing to deliver them to the next generation of computer technicians and forensic investigators. ■

The Internet & Computer Forensics

The increase in Internet and computer related crime, has focused public attention on the apparent ease with which criminals can access computer systems and steal data. This has provoked international press comment on the way police forces, world wide, are dealing with electronic evidence.

Stories which hit the newspaper headlines are not, in any way, representative of the extent of Internet related crime. As public awareness of computers and the vulnerability of their operating systems becomes heightened, we will see a rise in computer crime related stories - but at the moment they are hardly front page news.

> ***There is a feeling that the victim is, in some way, at fault when a hacker breaches a system's defences - so Industry tends to adopt a policy of secrecy which is not helpful to investigators.***

Software piracy, data theft, phone phreaking (breaking into a phone company's computerised control system to obtain free calls), 'denial of service' attacks (where a person's telephone service is disconnected by a hacker via a hacked entry into a telephone company's computer system), and the various flavours of cryptographic system cracking (using computer programs to break password protection systems) are simply not interesting to the majority of people - yet they cost industry millions each year. It is time to raise awareness of the issues at stake and to adopt a common policy for dealing with unauthorised computer access.

IP Spoofing

In the early days of the Internet, there was little emphasis on security and verification of Specific identities was not considered important enough to warrant more than a reasonably secure numerical computer handshake system, which is why TCP/IP (Transmissions Control Protocol / Internet Protocol) was adopted as the 'industry standard'.

TCP/IP is still the most commonly used protocol today, and still offers the same potential to an attacker. If a computer with an identifying set of numbers (known as an IP address) is set up to accept traffic from another similarly equipped, but remote, machine, then the chances are very good that the remote machine is authorised to access data. A person wishing to steal data from the data holding machine, only has to program their own machine to impersonate the authorised remote machine to gain access to data. This process is known as 'IP Spoofing'.

Problems faced by Investigators

Firewall technology, password protection and other data security systems are vital to prevent the theft or destruction of sensitive data, but they are subject to a degree of resistance from users who object to the perceived 'extra effort' needed to implement them.

> ***The problem is enhanced by the general inability of the Internet community to track attackers and present electronic evidence in a way that an average law court can understand and accept.***

It is one thing to present electronic evidence to an expert who can grasp the finite, yet conclusive, details that make a computer file evidence; it is quite another to show that evidence to a lay person and expect them to understand technology which is at the cutting edge of an expert's understanding.

Internet Service Providers (ISPs) have access to vast amounts of data from their machine logs - these, generally, list all users logged on at a specific time and what they are logged into. Electronic record keeping has never been an ISPs priority - they are, after all, running a service, and have plenty of problems just doing that.

Because of the pressures involved in running an ISP, an investigator may be fooled into thinking that ISP management are generally unco-operative. It is rarely the situation - they simply have better things to do than go through literally thousands upon thousands of records to find the single piece of information that could prove or disprove a case.

If they are approached in the right way, however, an investigator may get invaluable help from an ISP as many have the ability to run search software over their user records and machine logs. Most have an excellent knowledge of Internet software and can help to pinpoint specifics within that software which may help an investigation.

Electronic mail, for example, is becoming a major source of information for forensic investigators. Each mail is automatically time stamped by the computer system and has the potential to substantiate or disprove statements made by persons under investigation. It is very important to look at the whole mail document, as valuable data is frequently found in the header which some mail packages remove from the screen display.

Study the criminal to find the solution

It may be helpful to study the case of Kevin Mitnick, who was described by the New York Times as the most notorious cyber criminal in the US. Mitnick's motive for his computer crimes was not purely theft, but also vandalism. Mitnick enjoyed making his victims suffer and delighted in taunting them after violating their computer systems.

In an attempt to gain access to certain computer programs which would have given him the ability to hack into more sensitive data, Mitnick made the mistake of breaking into a computer network belonging to Tsutomu Shimomura, a leading US based Unix computer security expert. ▶

Unix 'finger' command

The break-in started with a Unix 'finger' command, issued by Mitnick, and designed to give him information about the system under attack. This is a standard exploratory feature used on the Internet to gain information about another computer connected to a network.

Shimomura became suspicious and began monitoring the suspect machine. By referring to the machine log he was able to list all abortive entry attempts, note the times that these attempts took place, and make notes of the aliases used by the attacker. The results of that monitoring are available on his WWW page at www.takedown.com. This web page gives detailed data pertaining to the attacks and gives a detailed breakdown on the techniques used to identify the intruder, but is also an advertisement for Shimomura's book, *Takedown*.

Use of Packet Filters (Sniffers)

Networks have been a target for illicit activity since criminals began using packet filters (or sniffers) to monitor traffic flowing through a network. It is possible for a packet filter user, with access to a network, to download this traffic without the knowledge of the other network users and de-code it to uncover passwords and other useful data.

> ***The packet filter was developed as a tool for network managers to discover who was accessing their systems and what sort of data was passing through them; however, the technology has been viewed by many as an invasion of privacy. In the hands of a skilled hacker it is rather more than that, as it provides the means to extract data with little risk of discovery.***

One piece of software reputedly stolen by Mitnick was, according to privacy activist John Gilmore, the latest version of the Berkeley Packet Filter for the U.S. military. This new filter was designed to be virtually undetectable on a UNIX system. Hidden deep in the system's kernel, it can pick up packets from the net and send them to any other computer on the network. This filter, apparently, can run at the astounding rate of more than 100,000 packets per second, which is particularly impressive when it is considered that few standard networks transmit more than a few dozen packets per second.

Mitnick then attempted to access other networked machines using the same TCP/IP weakness that had allowed him to gain control of Shimomura's computer. These protocols had been developed in the late 1970s and early 1980s to loosely identify Internet users. They were not designed to verify specific user identities.

Storage of stolen data

Mitnick began a campaign of attacks against the computer and telephone industries which gave him access to vast amounts of digital data. He chose to store this in computers, to which he had gained unauthorised access via the Internet. He trusted that the stolen data would go unnoticed alongside the computer's legitimate digital contents.

Moving data across the Internet is a common enough activity, but as hard disk storage space costs money, it is not too surprising that some of Mitnick's caches were discovered. A routine message from a system administrator asking that an abnormally large amount of data be removed, as it was contravening agreed practice, was enough to alert one user that his account had been compromised.

Note file sizes

An abnormality concerning file storage size is a reasonable indicator that something is amiss with a system's security. An intruder would not know the approved size of storage files and can easily contravene internal network regulations by dumping quantities of stolen files in space allocated to a hacked account. These stolen files provide the computer forensic teams with a wealth of knowledge as it is possible to identify when they were moved to a specific location, and sometimes, from where they were moved.

Watch the system clock

It is frequently possible to identify the time at which a file was deposited into a system. This is because many systems have an automatic process which updates file data if that file is accessed. If the recipient system's clock is accurate, or can be identified as being either fast or slow, then the exact time and date when a file was deposited can be established. This can provide a useful indication of when a crime was committed.

It was established that Mitnick was launching his attacks from a mobile phone attached to a computer. The phone had been cloned to access a legitimate mobile telephone user's account, but this information was quickly uncovered, so Shimomura was able to concentrate upon the computerised aspects of the case rather than trying to track Mitnick through the telephone networks.

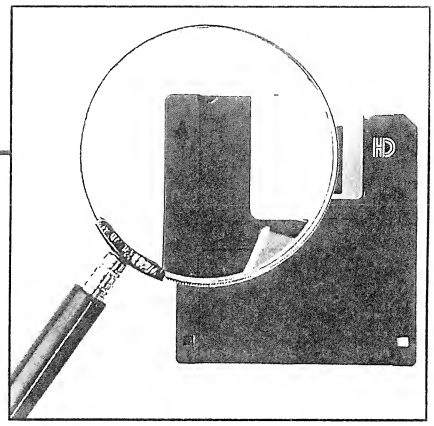
By concentrating on the electronic evidence contained within e-mail messages, system logs and telephone company records, it was possible to isolate the source of unauthorised computer access. This was later confirmed by a forensic investigation into the log on Mitnick's own notebook computer.

Almost all computer crime leaves a trail of electronic evidence behind it. The senior investigator's task is to ensure that this evidence is not destroyed by lack of knowledge. Operatives who deal with computer crimes need adequate training to ensure that sensitive data is not compromised. In the case of Kevin Mitnick, important evidence was destroyed by clumsy handling of system data by Shimomura's assistant, which slowed attempts to locate and arrest the perpetrator.

The use of correct forensic procedures would have prevented file damage and provided the courts with admissible evidence.

Ray Hatley

Forensic Q&A



To commence what will be a regular feature, here are answers to some frequently asked questions. The answers are not necessarily definitive - we hope that those printed here and in future issues will stimulate discussion. We look forward to receiving your questions and comments.

Q *If, during a raid, we find a computer which is switched on what is the correct handling procedure?*

A The keyboard should not normally be used to power down a suspect machine since this could trigger a logic bomb deliberately set within the system to destroy data. It is also possible that the defence could later accuse the investigating officers of altering information during the power-down and thus invalidating evidential integrity. For similar reasons no suspects should be allowed to touch the computer.

The general rule is that the computer should be switched off by the investigating officers using the main power switch. It is theoretically possible for this action to cause data damage but in practice this has never been known to occur. There are exceptions to the general rule such as when it is necessary to know what work was being carried out on the computer at the time of seizure. In this event the work should be carried out by a forensically competent person and a full record maintained of the actions performed.

Q *We have seized a computer during a raid. We don't have any facilities for storage of computer equipment. How can we preserve evidential continuity and integrity?*

A The equipment should be placed in clear plastic evidence bags securely fastened with numbered seals. Ideally storage should be in a temperature and humidity controlled environment. In practice this is rarely possible. As a minimum try to ensure that storage is within normally acceptable office working conditions. If a separate room is not available keep the equipment in a locked cupboard. Each time the equipment is accessed the old seal should be cut and placed in the evidence bag and a new seal fixed on completion. A full record should be kept of all persons having access to the equipment and of the actions taken.

Q *I am concerned that an individual in my company is mis-using his PC. What action should I take?*

A First of all don't let him know of your suspicions; he may try to destroy any evidence which is on the machine. Contact an outside organisation that offers computer forensic services and arrange to have an image copy made of the suspect machine. This will probably need to be a covert operation completed outside of normal office hours. The image copy will provide a "snap-shot" of the machine at a particular point in time. This can be examined for any un-authorised material. It can also be retained for a period and compared with a second copy taken at a later date, possibly after the suspect has been alerted of your concerns. The differences between the two copies may highlight the areas in which mis-use has taken place.

Q *I have seized several hundred floppy disks. How should I examine them?*

A It is essential in all computer forensic examination that analysis is only carried out on copies of suspect material. The write protect tag should therefore be set on each floppy disk and a copy made. The copy can be to another floppy disk using the DOS DISKCOPY command or it can be to an exact image file located on a hard or optical disk using dedicated forensic software. With any quantity of floppy disks greater than 10 the latter option is always preferable since it enables high speed search and other analysis techniques to be easily carried out. With any quantity of floppy disks in excess of 150 it is the only method by which efficient analysis can be undertaken.

Q *I've tried to make a copy of a seized computer but it has a password set in BIOS. How can I get around this?*

A There are three ways to circumvent a BIOS password. Firstly you can disconnect the battery, located on the motherboard, that supplies power to the BIOS to maintain user configured settings, including passwords. Secondly you can find the jumper or switch located on the motherboard that will disable the password. Finally you can remove the hard disk from the password protected machine and place it in another non-password protected machine such as a forensic workstation. The latter is the method used in 99% of cases. ■

Please address your questions and / or comments to:

Forensic Q&A
IJFC, Third Floor, Colonnade House
High Street, Worthing, West Sussex
U.K. BN11 1NZ.
e-mail: ijfc@pavilion.co.uk

Readers are advised to seek independent specialist advice before commencing an investigation.

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Noticeboard'. We reserve the right to edit if required.

EVENTS

WebSec '97

25-27 February, London
Optional Workshops: 24 & 28 February

Conference on Web, Intranet and Internet Security including Practical Solutions by Expert Faculty from BT, Mondex International, the Forensic Fraud Group of Deloitte Touche, University of Massachusetts Medical Center and other leading organisations.

In a special session, the conference will also feature a "face-off" between Robert Schifreen, famous for the Prestel break-in, and the man who arrested him, former Detective Inspector John Austen, previously Head of the Computer Crime Unit at New Scotland Yard. There will also be product solutions from leading vendors as well as in-depth workshops.

Contact: MIS Training Institute, London.
Tel: +44 (0)171779 8944
Fax: +44 (0)171779 8293

NET LAW - UK Legal Internet Symposium '97

26 February, London
Contact: Unicom Seminars Ltd, Middlesex, UK
Tel: + 44 (0)1895 256484
Fax: +44 (0) 1895 813095

International Forensic Science and Justice

The Forensic Science Society - 2nd Joint Meeting with the California Association of Criminalists
9-12 July, Harrogate, UK
Contact: Anne Holdsworth, The Forensic Science Society, UK
Tel: +44 (0)1423 506068
Fax: +44 (0) 1423 566391

In October last, the **International Conference on Money Laundering** was held in Rome to discuss Cyberpayments, Global Mafias, Offshore Investments, Securities, Corporate Security and International Financial Crimes.

To purchase documentation please contact the organisers:
D & D Communication Conference Division, Via Crocefisso,
21 - 20122 Milan, Italy.
Tel: +392583061 65

9th Computer Security Incident Handling Workshop

22-27 June, Bristol, UK

The annual FIRST Conference and Workshop is the only event of its kind. It focuses on the field of computer security incident handling and response. The presentations are international in scope and include the latest in incident response and prevention, vulnerability analysis, and computer security.

Contact: UKERNA
Tel: +44 (0)1235 822236
Fax: +44 (0) 1235 822399

The Forum of Incident Response and Security Teams (FIRST), is an international organisation that brings together a variety of computer security incident response teams from government, commerce and academia.

Further information about the FIRST organisation is available at the FIRST WWW server http://www.first.org/.

TRAINING

Computer Crime - Incident Handling & Investigations

15-17 April, Lincolnshire, UK
Contact: Computer Crime Consultants Ltd
Tel & Fax: +44 (0)1737 550093

Training in Computer Forensics

Four modules comprising:
Fundamental Computer Forensics
Applied Computer Forensics
Advanced Computer Forensics
Legal and Procedural Computer Forensics

Courses held monthly in West Sussex.

Contact: Computer Forensics Ltd
Tel: +44 (0) 1903 823181
Fax: +44 (0) 1903 233545

NEWS

To be reviewed in next month's issue *Computer Evidence: A Forensic Investigations Handbook* by Edward Wilding, Network Security Management Limited, published by Sweet and Maxwell. This is the first book to be published in the UK on computer forensic law. It gives:

- An outline of the legal issues involved in obtaining and presenting computer evidence
- Detailed guidance for collating and analysing evidential data
- Instructions in the use of investigative software and hardware
- An examination of the ways computers can be used to defraud, and how to investigate computer misuse
- Diagrams, screen dumps, printouts and photographs to illustrate key points

Denmark

The National Commissioners Serious Crime Squad has recently set up a programme to train 16 police officers to work in an EDP environment. The training, which is primarily conducted by IBM and Telecom Denmark, includes segments on operating systems, platforms, hardware, software, network, search and mobile phones. Upon completion of the course in March the officers will return to their different departments within the national police force.

International Journal of FORENSIC COMPUTING

Published by
Computer Forensic Services Ltd.
Third Floor, Colonnade House
High Street, Worthing, West Sussex
U.K. BN11 1NZ.
Tel: +44 (0) 1903 823181
Fax: +44 (0) 1903 233545
e-mail: ijfc@pavilion.co.uk